



Security Bulletin: IBM Aspera Console has addressed multiple vulnerabilities.

Security Bulletin

Summary

This Security Bulletin addresses multiple vulnerabilities that have been remediated in IBM Aspera Console 3.4.5.

Vulnerability Details

CVEID: [CVE-2024-40725](https://exchange.xforce.ibmcloud.com/vulnerabilities/298128) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/298128>)

DESCRIPTION: Apache HTTP Server allow a remote attacker to obtain sensitive information, caused by an incomplete fix for CVE-2024-39884 related to ignoring some use of the legacy content-type based configuration of handlers. By using AddType, an attacker could exploit this vulnerability, resulting in source code disclosure of local content.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/298128>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/298128>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2022-43850](https://exchange.xforce.ibmcloud.com/vulnerabilities/239226) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/239226>)

DESCRIPTION: IBM Aspera Console is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.

CVSS Base score: 4.6

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/239226>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/239226>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N)

CVEID: [CVE-2022-43840](https://exchange.xforce.ibmcloud.com/vulnerabilities/239077) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/239077>)

DESCRIPTION: IBM Aspera Console is vulnerable to an XPath injection vulnerability, which could allow an attacker to exfiltrate sensitive information from the application through the use of the XML

About cookies on this site

Our websites require some cookies to function properly (Required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your [cookie preferences](#) options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#) (<https://www.ibm.com/privac>

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

Accept all

Required only

CVEID: [CVE-2022-43851](https://exchange.xforce.ibmcloud.com/vulnerabilities/239227) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/239227>)

DESCRIPTION: IBM Aspera Console uses weaker than expected cryptographic algorithms that could allow an

attacker to decrypt highly sensitive information.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/239227>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/239227>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2024-39573](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/296120>)

DESCRIPTION: Apache HTTP Server is vulnerable to server-side request forgery, caused by a flaw in the mod_rewrite. By sending a specially crafted request, an attacker could exploit this vulnerability to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/296120>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/296120>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: [CVE-2024-39884](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/297177>)

DESCRIPTION: Apache HTTP Server allow a remote attacker to obtain sensitive information, caused by a regression in the core related to ignoring some use of the legacy content-type based configuration of handlers. By using AddType, an attacker could exploit this vulnerability resulting in source code disclosure of local content.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/297177>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/297177>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2018-25032](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/222615>)

DESCRIPTION: Zlib is vulnerable to a denial of service, caused by a memory corruption in the deflate operation. By using many distant matches, a remote attacker could exploit this vulnerability to cause the application to crash.

CVSS Base score: 7.5

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/222615>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/222615>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2023-27272](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/248496>)

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#) (<https://www.ibm.com/privacy>)

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

DESCRIPTION: Apache HTTP Server is vulnerable to a denial of service, caused by a NULL Pointer dereference flaw when serving WebSocket protocol upgrades over a HTTP/2 connection. By sending a specially crafted request, a remote attacker could exploit this vulnerability to crash the server process and degrade

performance.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/296128>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/296128>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: [CVE-2024-38472](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/296127>)

DESCRIPTION: Apache HTTP Server is vulnerable to server-side request forgery, caused by improper validation of WIndows UNC. By sending a specially crafted request, an attacker could exploit this vulnerability to leak NTML hashes to a malicious server.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/296127>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/296127>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2024-38476](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/296123>)

DESCRIPTION: Apache HTTP Server allow a remote attacker to obtain sensitive information, caused by improper input validation by the backend applications response headers. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, perform server-side request forgery attack or local script execution.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/296123>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/296123>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: [CVE-2015-4000](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/103294>)

DESCRIPTION: The TLS protocol could allow a remote attacker to obtain sensitive information, caused by the failure to properly convey a DHE_EXPORT ciphersuite choice. An attacker could exploit this vulnerability using man-in-the-middle techniques to force a downgrade to 512-bit export-grade cipher. Successful exploitation could allow an attacker to recover the session key as well as modify the contents of the traffic. This vulnerability is commonly referred to as "Logjam".

CVSS Base score: 4.3

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/103294>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/103294>) for the current score.

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#) (<https://www.ibm.com/privacy>)

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

CV ID: [CVE-2024-38452](#) (<https://exchange.xforce.ibmcloud.com/vulnerabilities/239228>)

DESCRIPTION: IBM's Aspera Connect client is vulnerable to a server-side request forgery (SSRF) attack. An attacker could exploit this vulnerability to send a specially crafted request to a remote server, causing the server to leak sensitive information in HTTP headers that could be used in further attacks.

CVSS Base score: 5.3

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/239228>

(<https://exchange.xforce.ibmcloud.com/vulnerabilities/239228>) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVEID: [CVE-2022-43847](https://exchange.xforce.ibmcloud.com/vulnerabilities/239168) (https://exchange.xforce.ibmcloud.com/vulnerabilities/239168)

DESCRIPTION: IBM Aspera Console is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.

CVSS Base score: 5.4

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/239168>
(https://exchange.xforce.ibmcloud.com/vulnerabilities/239168) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

CVEID: [CVE-2024-38473](https://exchange.xforce.ibmcloud.com/vulnerabilities/296126) (https://exchange.xforce.ibmcloud.com/vulnerabilities/296126)

DESCRIPTION: Apache HTTP Server could allow a remote attacker to bypass security restrictions, caused by an encoding flaw in mod_proxy. By sending specially crafted requests with incorrect encoding an attacker could exploit this vulnerability to bypass authentication validation.

CVSS Base score: 5.3

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/296126>
(https://exchange.xforce.ibmcloud.com/vulnerabilities/296126) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: [CVE-2022-43845](https://exchange.xforce.ibmcloud.com/vulnerabilities/239166) (https://exchange.xforce.ibmcloud.com/vulnerabilities/239166)

DESCRIPTION: IBM Aspera Console could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie.

CVSS Base score: 3.7

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/239166>
(https://exchange.xforce.ibmcloud.com/vulnerabilities/239166) for the current score.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVEID: [CVE-2024-40898](https://exchange.xforce.ibmcloud.com/vulnerabilities/298127) (https://exchange.xforce.ibmcloud.com/vulnerabilities/298127)

DESCRIPTION: Apache HTTP Server is vulnerable to server-side request forgery, caused by an error on Windows with mod_rewrite in server/vhost context. By sending a specially crafted request, an attacker could exploit this vulnerability to leak NTLM hashes to a malicious server.

CVSS Base score: 5.9

CVSS Temporal Score: See: <https://exchange.xforce.ibmcloud.com/vulnerabilities/298127>
(https://exchange.xforce.ibmcloud.com/vulnerabilities/298127) for the current score.

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/privac) (https://www.ibm.com/privac

y)

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

Version(s)

3.4.0 - 3.4.4


It is recommended that customers upgrade to the latest version of IBM Aspera Console:

Product(s)	Fixing VRM	Platform	Link to Fix
IBM Aspera Console	3.4.5	Windows	click here (https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=ibm%7EOther%20software&product=ibm/Other+software/IBM+Aspera+Console&release=All&platform=Windows&function=fixId&fixids=ibm-aspera-console-3.4.5.132-d94da33-windows-32&includeRequisites=1&includeSupersedes=0&downloadMethod=http)
IBM Aspera Console	3.4.5	Linux	click here (https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=ibm%7EOther%20software&product=ibm/Other+software/IBM+Aspera+Console&release=All&platform=Linux&function=fixId&fixids=ibm-aspera-console-3.4.5.31-65f2112.x86_64&includeRequisites=1&includeSupersedes=0&downloadMethod=http)

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

-  Subscribe to [My Notifications](#) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

References

- [Complete CVSS v3 Guide](#) 
- [On-line Calculator v3](#) 

Related Information

[IBM Secure Engineering Web Portal](#) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)

[IBM Product Security Incident Response Blog](#) (<http://www.ibm.com/blogs/psirt>)

About cookies on this site		
Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.	For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's privacy statement (https://www.ibm.com/privacy)	To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed here .

*This assessment Score is specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Cross-reference information

Product	Component	Platform	Version
IBM Aspera		Linux; Windows	1.0
IBM Aspera Console		Linux; Windows	3.4.2 PL7
IBM Aspera Enterprise		Linux; Windows	1.0
IBM Aspera Enterprise On Demand		Linux; Windows	1.1
IBM Aspera on Demand		Linux; Windows	1.0

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.	For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's privacy statement (https://www.ibm.com/privacy)	To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed here .
---	---	---

Document number:

7169766

Modified date:

23 September 2024

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/privacy) (<https://www.ibm.com/privacy>)

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).